

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri**In the Matter of the Search of**Eight Cellular telephones described in Attachment A, for
evidence described in Attachment B (List of
information/items to be seized) currently being held as
evidence located within the Eastern District of Missouri.

)

)

)

)

)

)

Case No. 4:21 MJ 3331 - 1-8 (NCC)

) SUBMITTED TO THE COURT AND

) SIGNED BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, JASON DIETL, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:
Eight Cellular telephones that are described in Attachment A, for evidence described in Attachment B (List of information/items to be seized) currently being held as evidence located within the Eastern District of Missouri,

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

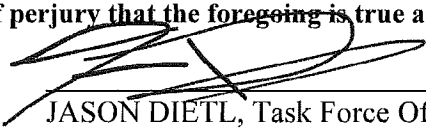
*Code Section**Offense Description*

Title 21, U.S.C., §§ 846, 841(a)(1)

Conspiracy to possess with intent to distribute controlled substance(s)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.**I state under the penalty of perjury that the foregoing is true and correct.**

 JASON DIETL, Task Force Officer
 Drug Enforcement Administration
Printed name and title

Sworn to, attested to, and affirmed before me via
 reliable electronic means pursuant to Federal Rules of
 Criminal Procedure 4.1 and 41.

Date: December 9, 2021City and State: St. Louis, MO

 Noelle C. Collins, U.S. Magistrate Judge
 AUSA: STEPHEN CASEY
Judge's signature

Noelle C. Collins, U.S. Magistrate Judge

Printed name and title

AUSA: STEPHEN CASEY

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)	Case No. 4:21 MJ 3331 - 1-8 (NCC)
EIGHT ELECTRONIC DEVICES AS)	
FULLY DESCRIBED IN ATTACHMENT A)	FILED UNDER SEAL
)	SUBMITTED TO THE COURT AND
)	SIGNED BY RELIABLE ELECTRONIC
)	MEANS
)	

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A SEARCH WARRANT

I, Jason Dietl, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the electronic devices described in Attachment A, currently in law enforcement possession, and the extraction from those devices of electronically stored information described in Attachment B.

2. I am a Task Force Officer with the Drug Enforcement Administration, and have been since August 2018. During my law enforcement career, I have participated in approximately 100 investigations involving the possession, manufacture and distribution of controlled substances. Those investigations have included the use of surveillance of persons involved in the possession and distribution of controlled substances, and the execution of arrest and search warrants for persons and places connected with the possession, manufacture and distribution of controlled substances. My specialized training has included, but is not limited to investigation of the manufacture, possession and distribution of controlled substance listed within the Controlled Substance Act, executing search and arrest warrants involving drug offenses, gathering drug and

non-drug evidence, under cover assignments, supervision and utilization of informants, narcotic smuggling, and money laundering.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 21, U.S.C. §§ 841 and 846 have been committed by Daveon BARNES, or other persons known and unknown. There is also probable cause to search the electronic devices described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE

5. The property to be searched is five cellular phones packaged in DEA evidence bag SSEE #M000521221, identified as DEA evidence number N-79, seized from the residence of Daveon BARNES on October 19, 2021 and three cellular phones packaged in DEA evidence bag SSEE #S001347918, identified as DEA evidence N-82, seized from the vehicle of Daveon BARNES on October 19, 2021, more specifically identified as:

- a. a red Apple iPhone bearing IMEI number 356552106256951 (“Device #1”);
- b. a black Apple iPhone with a black case and bearing IMEI number 356474107734466 (“Device #2”);
- c. a blue Apple iPhone bearing IMEI number 355044566721667 (“Device #3”);
- d. a red Apple iPhone bearing IMEI number 351156784921590 (“Device #4”);
- e. a white Apple iPhone bearing IMEI number 356849113061097 (“Device #5”)

- f. described as a blue Samsung cell phone with a black case (“Device #6”);
- g. a grey Apple iPhone bearing IMEI number 354446066888667 (“Device #7”);
- and
- h. a white Apple iPhone with a red and black case, bearing IMEI number 356840116558072 (“Device #8”).

6. Device #1 through Device #8 (collectively “the Devices”) are currently located at the DEA St. Louis Division Office located at 317 South 16th Street, St. Louis, Missouri.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing

dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. A wireless telephone may have wireless connection capabilities such as Wi-Fi and Bluetooth.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets,

and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

9. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

PROBABLE CAUSE

10. In June 2020, DEA-St. Louis Division Group 28, and the United States Postal Inspectors Service (USPIS), initiated an investigation into the GRIFFIN drug-trafficking organization (DTO) which was distributing large quantities of fentanyl, heroin and crystal methamphetamine in the St. Louis, Missouri area. The investigation established that Stephen GRIFFIN was the head of the DTO. GRIFFIN established a large network of retail distributors and facilitators in order to engage and maintain his DTO's sale of narcotics. A significant portion of the narcotics were mailed through the United States Postal Service to various addresses within the St. Louis, Missouri area.

11. As part of the investigation, on May 3, 2021, investigators arrested Daveon BARNES after he retrieved a United States Postal Service (USPS) package, which had been delivered to 1225 Grogan Place, St. Louis, Missouri 63133, that investigators believed contained narcotics. This was based on investigators identifying, and seizing, other USPS delivered packages, which contained narcotics, that had been delivered to other members of the GRIFFIN DTO. BARNES was found to be in possession of approximately one kilogram of fentanyl, Oxycodone pills, marijuana, and three guns (one of which was a stolen AK-47 out of St. Louis, Missouri).

12. During the post-arrest interview, BARNES advised investigators that he was not a member of the GRIFFIN DTO and that he and Stephen GRIFFIN were actually enemies. BARNES claimed GRIFFIN blamed him for working with law enforcement which led to GRIFFIN being federally charged on a previous case.

13. On October 13, 2021, Daveon BARNES was federally indicted by a grand jury in the Eastern District of Missouri 4:21 CR554 SRC/NAB. An arrest warrant was issued for Daveon

BARNES arrest who investigators believed was residing at 863 Hazelvalley, Hazelwood, Missouri 63042.

14. On October 19, 2021, DEA Special Agent (SA) Andy Vineyard, and Hazelwood Police Sergeant Ryan Enge, established surveillance at 863 Hazelvalley, Hazelwood, Missouri 63042, awaiting the arrival of the USMS arrest team. During surveillance, SA Vineyard observed a white colored Lincoln 4-door sedan parked in the driveway. Task Force Officer (TFO) Dan Sanders notified investigators that BARNES, on October 18, 2021, had utilized the same Lincoln sedan to conduct a drug transaction with an undercover St. Louis County Drug Detective where BARNES exchanged suspect fentanyl for \$100.00 in Official Advanced Funds (OAF) from St. Louis County. St. Louis County Detectives later field tested the suspect fentanyl which yielded a positive test.

15. The USMS arrest team executed the arrest warrant at 863 Hazelvalley, Hazelwood, Missouri 63042, targeting BARNES. The arrest team knocked on the front door and made loud 'POLICE' announcements multiple times. After getting no response, the arrest team breached the front door and made entry into the residence. A female (identified as Dakenzie SHEPPERD), and her son, exited the residence and advised the arrest team that BARNES was located in the master bedroom of the residence. BARNES complied with directions from the arrest team and exited the house without incident.

16. SHEPPERD granted written consent to search the residence and the white Lincoln (bearing New York License Plate HYZ-3522) parked in the driveway. SHEPPERD advised SA Vineyard, and United States Postal Inspector (USPI) Jordan Wicks, that she had regular access to the vehicle and was able to drive it. SA Vineyard also stated that SHEPPERD had regular access to the residence and currently resides there. SA Vineyard, and USPI Wicks observed belongings (i.e.

clothing and children's toys), which appeared to be SHEPPERD's and her son's, throughout the residence.

17. Investigators conducted a search of the residence and located the following items in the listed locations:

a. Master Bedroom—SA Vineyard located two (2) firearms next to the bed, USPI Wicks located a large amount of U.S. currency inside BARNES' red colored jacket and inside a bag hanging on the side of the bed, a black colored electronic scale, and five (5) cellular phones near the bed, specifically Device #1 through Device #5;

b. Vehicle—USPI Wicks located a large amount of blue/clear capsules, containing an off white powder (suspect fentanyl) in a large clear plastic bag, a small plastic bag containing unknown white colored pills in the center console, and three (3) cellular phones in the glove box, specifically Device #6 through Device #8.

18. While packaging the U.S. Currency as evidence, SA Vineyard, as witnessed by DEA SA Kelly Gougher, located three (3) \$20 bills utilized by St. Louis County Detectives in the undercover purchase of fentanyl from BARNES on October 18, 2021. Matching serial numbers on the bills were identified by comparing them to a copy of a photograph of the St. Louis County OAF funds which were utilized during the purchase.

19. The St. Louis County Undercover Detectives also provided the phone number they utilized to make contact with BARNES to arrange said purchase of fentanyl. Investigators believe one of the seized cellular phones is the one BARNES utilizes in furtherance of his continued retail drug sales.

20. Based on my training and experience in such investigations, including electronic surveillance investigations, I and other members of the investigative team, know that drug

traffickers communicate with each other utilizing cellular telephones and other electronic devices to facilitate the overall scheme of their illicit endeavors. In order to be successful, drug traffickers must communicate via telephones or other electronic devices to orchestrate the importation of controlled substances; to manage and maintain contact with drug couriers; to maintain contact with lower level distributors in their day-to-day operations; to maintain contact with safe house operators where narcotics are stored; and to coordinate the return movement of the drug derived profits back to the sources of supply.

21. I also know based on my training and experience that individuals involved in the trafficking of narcotics use devices such as the subject electronic devices to facilitate their overall schemes and their illicit endeavors. In order to make it easier for drug currency and narcotics traffickers to communicate with one another, their phones and other devices often contain stored telephone numbers, programmed names, addresses, and encrypted codes and names.

22. I also know that the phones and other communication devices of narcotics traffickers often contain voicemails, text messages, photographs and emails relating to communications with co-conspirators, meeting locations as well as the telephone numbers of co- conspirators who have called or been called by the device.

23. Electronic devices and the services they provide are such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society. Thus, there is reason to believe that the individuals and their associates described in this affidavit used mobile electronic devices in conjunction with the events described herein. The devices themselves operate as instrumentalities of the crimes.

24. Based upon the preceding information, and my training and experience and that of my team, I believe Daveon BARNES and others are distributing fentanyl in violation of Title 21, United States Code, Sections 841(a)(1) and 846. Accordingly, my team and I believe that evidence of participation in drug trafficking will be found in Devices #1 through #8.

25. The Devices are currently in the possession of the DEA. In my training and experience, I know that the Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the device first came into the possession of the DEA.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

29. I seek a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

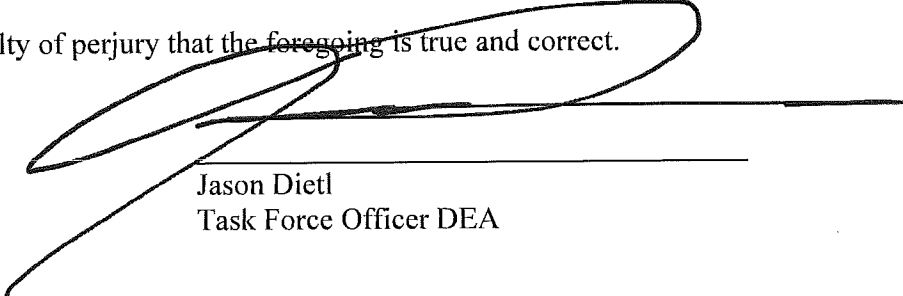
30. Because this warrant seeks only permission to examine the Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

31. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and

related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

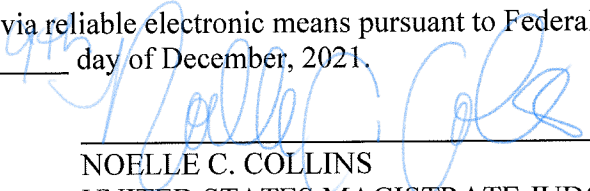
I state under the penalty of perjury that the foregoing is true and correct.

12/9/21
DATE



Jason Dietl
Task Force Officer DEA

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41, this 9th day of December, 2021.



NOELLE C. COLLINS
UNITED STATES MAGISTRATE JUDGE
Eastern District of Missouri

ATTACHMENT A

The property to be searched is:

- a. a red Apple iPhone bearing IMEI number 356552106256951 ("Device #1") **4:21 MJ 3331-1;**
- b. a black Apple iPhone with a black case and bearing IMEI number 356474107734466 ("Device #2") **4:21 MJ 3331-2;**
- c. a blue Apple iPhone bearing IMEI number 355044566721667 ("Device #3") **4:21 MJ 3331-3;**
- d. a red Apple iPhone bearing IMEI number 351156784921590 ("Device #4") **4:21 MJ 3331-4;**
- e. a white Apple iPhone bearing IMEI number 356849113061097 ("Device #5") **4:21 MJ 3331-5;**
- f. described as a blue Samsung cell phone with a black case ("Device #6") **4:21 MJ 3331-6;**
- g. a grey Apple iPhone bearing IMEI number 354446066888667 ("Device #7") **4:21 MJ 3331-7; and**
- h. a white Apple iPhone with a red and black case, bearing IMEI number 356840116558072 ("Device #8") **4:21 MJ 3331-8.**

The Devices are currently located at the DEA St. Louis Division Office located at 317 South 16th Street, St. Louis, Missouri.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 21 U.S.C. §§ 841 and 846 and involve Daveon BARNES, from January 1, 2021 to the present including:

- a. Lists of customers and related identifying information;
- b. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- d. Any information recording BARNES' schedule or travel;
- e. All bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.